



CVE-2021-25742

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-25742
State	PUBLIC
Assigner	security@kubernetes.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-29 04:15:00 UTC
Updated	2021-12-15 14:06:00 UTC
Description	A security issue was discovered in ingress-nginx where a user that can create or update ingress objects can use the custom

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kubernetes	Ingress-nginx	All	All	All	All
Application	Kubernetes	Ingress-nginx	1.0.0	All	All	All
Application	Netapp	Trident	-	All	All	All

References

Reference

- [CVE-2021-25742 Kubernetes Vulnerability in NetApp Products | NetApp Product Security](#)
- [CVE-2021-25742: Ingress-nginx custom snippets allows retrieval of ingress-nginx serviceaccount token and secrets across all namespaces · I](#)
- [\[Security Advisory\] CVE-2021-25742: Ingress-nginx custom snippets allows retrieval of ingress-nginx serviceaccount token and secrets across](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

Vendor Comments And Credit

Discovery Credit

LEGACY: Mitch Hulscher

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)